#2

FORM PTO-1449	SERIAL NO. 09/710,987	ATTORNEY DOCKET NO. 2944.2.1
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT (use several sheets if necessary)	FILING DATE November 8, 2000	GROUP ART UNIT
	APPLICANT(S): Richard Schroeppel	

REFERENCE DESIGNATION U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS/ SUBCLASS	FILING DATE
BD	A1	6,163,841	12/19/2000	Venkatesan et al.	713/176	06/23/98
	A2	6,141,420	10/31/2000	Vanstone et al.	380/30	01/29/97
BD	A3	5,982,895	11/09/1999	Dworkin et al.	380/9	12/24/97

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS/ SUBCLASS	TRANSLATION
BD	A4	98,302,286	10/28/1998	Europe	G06F 7/72	Yes

NON-PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT (Including Author, Title, Source, and Pertinent Pages)
BD	A5	Schroeppel, R. et al. "Fast Key Exchange with Elliptic Curve Systems," Advances in Cryptology- CRYPTO'95, 08/31/1995, pages 43-56.
	A6	Vanstone, S.A. et al., "Elliptic Curve Cryptosystems Using Curves of Smooth Order Over the Ring Zn," IEEE Trans. On Information Theory, vol. 43, no. 4, July 1994, pages 1231-1237.
BD	A7	Knudson, E., "Elliptic Scalar Multiplication Using Point Halving," Asiacrypt '99, 11/14/99, pages 134-149.

EXAMINER Bernard Dauden	DATE CONSIDERED 4/5/04

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through ci conformance and not considered. Include copy of this form with next communication to applicant(s).

#5

FORM PTO-1449	SERIAL NO. 09/710,987	ATTORNEY DOCKET NO. 2944.2.1
LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT	FILING DATE November 8, 2000	GROUP ART UNIT 2132
(use several sheets if necessary)	APPLICANT(S): Richard Schroeppel	

U.S. PATENT DOCUMENTS

EXAMINER INITIAL*		DOCUMENT NUMBER	DATE	NAME	CLASS/ SUBCLASS	FILING DATE
BP	B1	6,252,959	06/26/2001	Paar et al.	380/28	05/20/98
	B2	6,038,581	03/14/2000	Aoki et al.	708/492	01/28/98
	B3	5,892,912	04/06/1999	Suzuki et al.	~~395/200.48~~	10/29/96
	B4	5,812,438	09/22/1998	Lan et al.	~~364/746.1~~	10/12/95
	B5	5,805,703	09/08/1998	Crandall	380/30	11/27/96
BP	B6	5,442,707	08/15/1995	Miyaji et al.	380/30	09/27/93

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS/ SUBCLASS	TRANSLATION YES	TRANSLATION NO
BP	B7	WO 01/04742	01/18/2001	France	G06F 7/72		X
BP	B8	WO 96/04602	02/15/1996	Canada	G06F 7/72	X	

NON-PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT (Including Author, Title, Source, and Pertinent Pages
BP	B9	"Efficient Algorithms for Elliptic Curve Cyrptosystems," 1997 Jorge Guarjardo excerpt, Advances in Cryptology - Crypto 1997, ©1998 Springer-Verlag, pp. 242-356
	B10	"New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n," 1991Kenji Koyama excerpt, Advances in Cryptology - Crypto 1991, ©1998 Springer-Verlag, pp. 252-266
BP	B11	"Integer Division in Residue Number Systems," 1994 Hitz, M.A. and Kaltofen, E., excerpt IEEE Transactions on Computers, ©1995 IEEE, pp. 983-989

EXAMINER Beemnet Dada	DATE CONSIDERED 4/5/04

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not i and not considered. Include copy of this form with next communication to Applicant(s).